Meeting Summary

INFORMATION						
DATE:	09/16/2010	**START TIME:**	2:00pm	**END TIME**	4:00pm	**LOCATION:**	NH National Guard Army Aviation Support Facility

SUBJECT/ PROJECT:	New Hampshire Information Technology Council (IT Council)
PURPOSE:	Scheduled Meeting
CHAIRPERSON:	Lieutenant Colonel David Routhier, Director of Information Management, New Hampshire National Guard
ATTENDEES:	IT Council Members: Rebecca Landry, IMS Director, city of Keene; Lieutenant Colonel David Routhier, Director of Information Management, New Hampshire National Guard; IT Council Designees William Baggeroer, Dept. of Health & Human Services, Chief Information Office; Kevin P. O'Brien, Dept. of Safety, Chief of Policy & Planning; Michael Pillsbury, Dept. of Transportation, Deputy Commissioner; Charles Russell, Dept. of Administrative Services, Financial Data Management Director Guest Attendees: Kenneth Graf, UNH; Keith Lohmann, Dept. of Safety, J-One Project Manager; David Reilly, Microsoft, NH Account Executive; Laurie Carey, Microsoft, Technology Strategist; Amy Marchibroda, Microsoft, Account Executive Department of Information Technology Staff: Rebecca Bolton, IT Manager, Agency Software Division; Theresa Pare-Curtis, Director, Web Support Division; Sally Gallerani, Director, Technical Support Services Division; Gail Hambleton, IT Manager, Agency Software Division; Peter C. Hastings, Interim Chief Information Officer/Commissioner; Mary Houde, Assistance Director, Agency Software Division; Wendy Poulliot, Assistance Director, Operations Division; Jerry Romano, IT Manager, Technical Support Services; Leslie Williams, Manager, Information Technology Security Group

	ABSENTEES:	Art Durette, NH Association of Counties Representative, Deputy Sherriff Hillsborough County; Nina Gardner, Judicial Council, Executive Director; George N. Campbell, Jr, Dept. of Transportation, Commissioner; Kevin Clougherty, Dept. of Revenue Administration, Commissioner; Thomas B. Getz, Public Utilities Commission, Chairman; Linda Hodgdon, Dept. of Administrative Services, Commissioner; Senator Deborah Reynolds, District 2; Earl M. Sweeney, Dept. of Safety, Assistant Commissioner; Nicholas Toumpas, Dept. of Health and Human Services, Commissioner; Representative Charles Townsend, Grafton County; Science, Technology and Energy Committee

ITEM #	AGENDA
1.	Welcome and Introduction of Meeting Attendees, David Routhier
	Meeting Minute Approval, July 15, 2010 Meeting
2.	Demonstration of NHView and NHGuardView GIS projects
3.	Microsoft: Information Security Risk related to legacy software
4.	Cyber-security in NH State Government
5.	Cyber-security at UNH

ITEM #	MINUTES
1.	LTC David Routhier welcomed the IT Council Members and Guests and introduced meeting attendees. The July 15, 2010 Meeting Minutes were approved once there was a quorum.
2.	**Demonstration of NHView and NHGuardView GIS projects** LTC David Routhier gave a demo of NHView and NHGuardView which are two GIS-based applications. A short presentation was given on a few other GIS solutions being used by School Boards, Firefighters, and Police. Discussion Points: • The major question has been, what GIS data can be shared? • The sharing of data and collaboration improved following the July 15, 2010 IT Council Meeting. • There has been significant progress with NHView and NHGuardView in the last few months. • Assistant Director Houde asked if there is a GIS Steering Committee. • Director O'Brien explained that the Department of Revenue is working with Emergency 911 to gather GIS data. • Interim CIO Hastings added that a number of Commissioners are working on a Memorandum of Agreement related to sharing GIS data. • LTC Routhier commented that Sean Goodwin, Emergency 911, is currently working with other States' on sharing GIS information.
3.	**Microsoft: Information Security Risk related to legacy software** David Reilly, Laurie Carey, and Amy Marchibroda of Microsoft gave a presentation on Microsoft's Security offerings. Discussion Points: • January 15, 2002, Microsoft made a commitment to a dramatic shift in the company's mission and strategy – to focus on making more secure and reliable products and services, protecting their customers' privacy, and being more transparent and responsive in their business practices.

3. continued	• Microsoft products are designed with integration and end-to-end coverage in mind. Each product from collaborative tools like Microsoft Exchange to operating systems like Windows 7, security is a top priority. Common security management tools provide end users a familiar set of set up and management adjustments, and IT professionals an integrated methodology for managing security across the enterprise.
	• The Core Infrastructure Optimization model is focused on demonstrating how the Microsoft core-infrastructure solutions are the best investment to reduce IT costs while still ensuring that IT is aligned with and driving the business. The number-one priority for many businesses is maximizing the <u>value</u> of IT.
	• The new model is comprised of the following four capabilities:
	    • **Datacenter Services** including Datacenter Management and Virtualization, Server Security, Networking, and Storage.
	    • **Client Services** including Client Management and Virtualization, Mobile Device Management, and Client Security.
	    • **Identity and Security Services** including Identity and Access, Security Management, and Information Protection and Control.
	    • **IT Process** including End-to-end Process (Information Technology Infrastructure Library and Microsoft Operations Framework).
	• As government looks to address strategic and tactical issues to drive cost reductions and provide additional services, they face a mix of challenges and opportunities that are complicated by pressures from a changing threat landscape and the inadequacies of existing security solutions.
	• In response to these business challenges and opportunities, Microsoft is taking a fundamentally different approach to security. They call it **Business Ready Security**.
	• Microsoft delivers a comprehensive, user-centric approach to protection and access that helps organizations protect virtually everywhere by providing defense in depth across multiple layers.
	• Spam was once just an annoyance, but it has become the tactic of choice for online deception, fraud, and abuse.
	• As part of the Business Ready Security strategy, Microsoft Forefront security products are made available through a comprehensive set of six solutions: Secure Datacenter, Secure Messaging, Secure Collaboration, Secure Desktop, Information Protection, and Identity and Access Management.

4.	**Cyber-security in NH State Government**
	
	LTC David Routhier gave a presentation regarding cyber security.
	
	Discussion Points:
	• Security must balance business requirements and controls.
	• Safeguarding the confidentiality, integrity and availability of information residing on state resources.
	• Threat landscape continues to evolve
	• Must manage residual, accepted, and deferred risks.
	• NH National Guard went to Department of Defense security conference in July.
	    • Most difficult threat is from internal employees, known as Social Engineering.
	• Dave Reilly of Microsoft mentioned the Federal Notification Law requirement whereby you must notify all individuals or potential security threats.
	• Deputy Commissioner Pillsbury asked why there has been a downward trend in viruses.
	    • Laurie Carey of Microsoft responded that management of Spam has improved. For example, an organization will be blacklisted quickly whereby they can not send out any email when they are suspected of being a Spammer.
	    • Director Landry added that hackers are using more sophisticated tools such as thumb drives.
	    • Jerry Romano explained that anti-spam tools contain connection control which prevents any connection whatsoever to some suspicious sites which is helping to drive the number of virus' down.

4. continued	• NH Army National Guard is acquiring EADS NA HOTSIMT to train network defenders on advanced concepts and techniques used to detect, recognize, identify, and mitigate network threats and vulnerabilities and how to report them. Using Hands-on Training Simulators (HOTSIMT), students operate and defend a network representative of the most common architectures. Students will demonstrate the ability to detect a network intrusion, recognize the attack type, identify the risk/threat to vulnerable devices, mitigate that threat, and report the incident.
5.	**Cyber-security at UNH** Ken Graf provided an overview of some cyber-security initiatives at UNH. • CS & IT programs growing • Students looking for internships/work study • Various local/regional/national competitions

ACTION ITEMS			
ITEM #	**DESCRIPTION**	**Assigned To**	**Due Date**
NEXT MEETING: TBD			